View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Croatian Digital Thesis Repository

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

KARIN OBROVAC

IPv6 ZA IoT

Završni rad

Pula, rujan 2018.

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

KARIN OBROVAC

IPv6 ZA IoT

Završni rad

JMBAG: 0303045931, redoviti student

Studijski smjer: Informatika

Kolegij: Osnove IKT

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijsko-komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: prof. dr. sc. Vanja Bevanda

Pula, rujan 2018.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani_____, kandidat za prvostupnika informacijsko- komunikacijske tehnologije ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli,_____, 2018 godine.

IZJAVA

o korištenju autorskog djela

Ja,_____dajem odobrenje

Sveučilištu Jurja Dobrile

u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom

_____

_____

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli,_____, 2018 godine.

Potpis

_____

SADRŽAJ

1. UVOD

Naslov završnog rada je IPv6 (Internet protokol verzije 6) za IoT (Internet stvari). Svrha rada je opisati IPv6 te njegove standarde koji se primjenjuju za komunikaciju Internet stvari. Pojam Internet stvari označava uređaje koji se spajaju te međusobno komuniciraju putem Interneta. Kako broj uređaja koji se spajaju na Internet, neprestano raste, raste i potreba za većim brojem IP adresa.

U drugom poglavlju riječ je o OSI i TCP/IP modelu te Internet protokolu verzije 4 (IPv4). Objašnjeno je što su to OSI i TCP/IP model, slojevi od kojih se navedeni modeli sastoje, njihova svtha te osnovne funkcije IPv4.

U trećem poglavlju riječ je IPv6 protokolu. Opisano je adresiranje i klasifikacija, navedeni su tipovi adresa tog protokola. Objašnjeno je zaglavlje paketa te fragmentacija i usmjeravanje paketa.

Četvrto poglavlje govori o Internet stvarima. Opisana je njihova primjena, prednosti i mane, komunikacija IoT uređaja te tehnologije koje IoT uređaji koriste.

Peto poglavlje opisuje značenje IPv6 za IoT. Navedeni su i opisani IPv6 standardi koje IoT koristi, naveden je IoT6 projekt te je opisana njegova arhitektura. Opisana je IPv6 sigurnost i naveden je IPSec protokol.

2. OPĆENITO O INTERNET PROTOKOLIMA

2.1 Slojevi OSI referentnog modela

"OSI (Open System Interconnection) referentni model je model strukture računalnog sustava koji omogućava međusobnu razmjenu sadržaja s drugim takvim sustavima."[1] OSI referentni model daje smjernice kod razvoja mrežnih protokola i komunikacije. Podijeljen je na sedam slojeva, gdje svaki sloj može sadržavati jedan ili više protokola. Podjelom na slojeve i pridržavanjem smjernica, ubrzava se razvoj protokola za svaki od slojeva. Svaki od slojeva opisuje skup međusobno povezanih funkcija koje omogućuju dio računalne komunikacije. Komunikacija unutar modela provodi se na način da određeni sloj koristi usluge razine ispod, a pruža usluge razini iznad sebe. Slojevi su sačinjeni na način da promjena na jednom sloju ne zahtjeva promjenu na ostalim slojevima. OSI model obično se opisuje od najnižeg sloja.

1. **Fizički sloj (Physical layer):** Najniži je sloj OSI referentnog modela i ujedno i jedini sloj koji se bavi fizičkim prijenosom podataka. Detalji rada kablova, konektori, bežični radio prijenosnici, kartice mrežnog sučelja te ostali hardverski uređaji su funkcija fizičkog sloja. Fizički sloj odgovoran je za raznovrsna šifriranja i signalne funkcije koji pretvaraju podatke iz bitova u signale koji se mogu dalje prenositi mrežom. Ovaj je sloj usko povezan sa podatkovnim slojem.[2]
2. **Podatkovni sloj (Data Link layer):** Podatkovni sloj je drugi najniži sloj OSI modela. Njegove su zadaće povezanost i odabir putanje između uređaja, pristupanje mediju za prijenos podataka, te otkrivanje grešaka u prijenosu preko fizičkog sloja.
3. **Mrežni sloj (Network layer):** Treći najniži sloj OSI referentnog modela je mrežni sloj. Da bi paketi stigli do odredišta, trebaju proći kroz nekoliko usmjerivača. Mrežni sloj povezuje i odabire najbolju putanju za usmjeravanje paketa od izvora do odredišta. Kako navodi Kozierok, neki od zadataka koje izvodi mrežni sloj su logičko adresiranje, usmjeravanje, enkapsulacija datagrama, fragmentacija i ponovno sastavljanje te rješavanje problema i dijagnostika. Najčešće korišteni protokol mrežnog sloja je Interent protokol (IP).

[1] Mario Radovan., Računalne mreže (1), Rijeka, 2010. str. 22
[2] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 102

4. **Transportni sloj (Transport layer):** Često nazivan srednjim slojem, transportni sloj je četvrti sloj OSI referentnog modela. Transportni sloj podatke koje dobiva od sloja sesije razbija u manje jedinice te ih zatim predaje nižem, mrežnom sloju.

Dva najznačajnija protokola transportnog sloja su:

1. Protokol kontrole prijenosa (TCP – engl. Transmission Control Protocol): „Osnovni je protokol transportnog sloja OSI modela te je odgovoran za uspostavljanje i upravljanje vezom, te pouzdanim prijenosom podataka između softverskih procesa i uređaja.“[3]
2. Podatkovni protokol korisnika (UDP – engl. User Datagram Protocol): „Jednostavan protokol prijenosne razine koji aplikacijama omogućuje direktno korištenje usluga sa Internet razine.“[4] Mnogo je jednostavniji od TCP protokola, ali je isto tko i mnogo nesigurniji što se tiče prijenosa podataka

5. **Sloj sesije (Session layer):** Glavni zadaci sloja sesije su razmjena informacija u komunikaciji te alociranje memorije za pohranu podataka.

6. **Prezentacijski sloj (Presentation layer):** Zadatak prezentacijskog sloja je pretvaranje podataka u format kojeg aplikacijski sloj može podržati. Oblikuje i šifrira podatke koji će se slati mrežom, sprječavajući probleme sa kompatibilnošću.[5]

7. **Aplikacijski sloj (Application layer):** Poslijednji je sloj OSI referentnog modela te izravno komunicira sa programskim aplikacijama ili s korisnikom. Na aplikacijskom sloju definirani su aplikacjski protokoli koji implementiraju određene korisničke aplikacije. Neki od najpoznatijih protokola na ovome sloju su: HTTP, FTP, SMTP, Telnet i dr.[6]

---

[3] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 122
[4] Mujarić, Eldis. 2009. „Računalne mreže“. Layer-x. http://mreze.layer-x.com/s040200-0.html
[5] Beal, Vangie. 2018. „The 7 Layers of the OSI Model“. Webopedia. https://www.webopedia.com/quick_ref/OSI_Layers.asp
[6] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 112

2.2 Slojevi TCP/IP modela

Godine 1969., Američka Agencija za napredne istraživačke projekte (ARPA – engl. Advanced Research Projects Agency) pokrenula je razvoj računalne mreže ARPANet koja je prethodila razvoju računalne mreže Internet. TCP/IP model sastoji se od mnogo različitih protokola od kojih su najznačajniji Protokol kontrole prijenosa (TCP) i Internet protokol (IP). Ova su dva protokola važna zbog toga što je većina najkritičnijih funkcija TCP/IP modela trećem i četvrtom sloju, gdje se TCP i IP protokoli i nalaze.[7]

TCP/IP model sastavljen je od četiri sloja: Sloja mrežnog sučelja, Internet sloja, Aplikacijskog sloja, Transportnog sloja, te Aplikacijskog sloja.

1. **Sloj mrežnog sučelja (Network Interface Layer):** Ovaj sloj odgovara fizičkom sloju i podatkovnom sloju OSI referentnog modela. Određuje detalje fizičkog prijenosa podataka mrežom. Prijenos podataka omogućuju bakrene žice, optička vlakna, odnosno elektromagnetski valovi ako se radi o bežićnoj komunikaciji. Na sloju mrežnog sučelja nalazi se LAN arhitektura Ethernet.

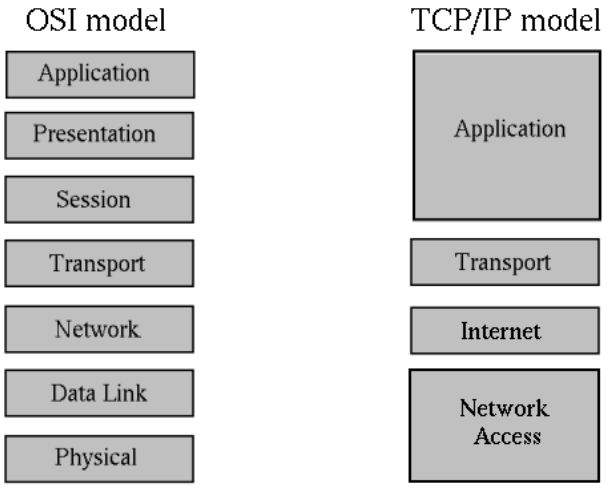
2. **Internet sloj (Internet Layer):** Drugi sloj TCP/IP modela je Internet sloj. Glavna odgovornost ovog sloja je pakiranje, adresiranje i usmjeravanje podataka koji se mrežom prenose do odredišta. Najznačajniji protokol na ovome sloju je IP (Internet protokol) koji je odgovoran za IP adresiranje, pakiranje i usmjeravanje podataka. Ostali protokoli na Internet sloju su ICMP (engl. Internet Control Message Protocol), ARP (engl. Address Resolution Protocol), IGMP (engl. Internet Group Managament Protocol) te RARP (engl. Reverse Address Resolution Protocol). Internet sloj odgovara mrežnom sloju OSI referentnog modela.

3. **Transportni sloj (Transport Layer):** Na trećem, transportnom sloju, nalaze se dva protokola: TCP (engl. Transmission Control Protocol) i UDP (engl. User Datagram Protocol). TCP protokol se koristi pri slanju onog sadržaja kojeg se želi prenijeti na pouzdan način. Ako se prilikom prijenosa paketa

[7] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str.122

izgube ili izvrnu podaci, TCP protokol neće zaprimiti te pakete nego će od pošiljatelja zahtijevati novi, ispravan prijenos. UDP protokol se koristi za prijenose gdje je brzina važnija od ispravnosti.[8]

4. **Aplikacijski sloj (Application Layer):** Posljednji sloj TCP/IP modela je aplikacijski sloj koji odgovara sloju sesije, prezentacijskom i aplikacijskom sloju OSI modela. Aplikacijama omogućuje međusobnu komunikaciju i pristup uslugama nižih slojeva. Najznačajniji protokoli na aplikacijskom sloju su HTTP (engl. HyperText Transport Protocol) koji određuje rad web sustava, te SMPT (engl. Simple Mail Transfer Protocol) koji je namijenjen za pouzdan prijenos računalne pošte.



Slika 1. Prikaz slojeva OSI referentnog modela i TCP/IP modela
Izvor: https://sysportal.carnet.hr/node/352

Slika 1 predstavlja slojeve u OSI referentnom modelu i TCP/IP modelu. Jedna od razlika između ta dva modela je u broju slojeva gdje ih OSI model ima sedam, a TCP/IP četiri.

[8] Mario Radovan., Računalne mreže (1), Rijeka, 2010. str. 26

2.3 Internet protokol verzije 4

Internet protokol (IP) je osnovni protokol Internet sloja TCP/IP modela, a koriste ga i protokoli na višim slojevima. IP protokol se smatra nepouzdanim protokolom jer protokoli na transportnom i palikacijskom sloju provjeravaju dosljednost podataka i detektiraju i ispravljaju greške.“[9]

Neke od osnovnih funkcija IP protokola su:[10]

- Definiranje sheme adresiranja na internetu
- Definiranje IP paketa
- Prosljeđivanje podataka između razine pristupa mreži i prijenosne razine
- Fragmentacija i sastavljanje paketa

Svako računalo koje se povezuje na Internet mora imati jedinstvenu brojčanu oznaku koja se naziva IP adresa. Trenutni standard IP adresiranja na internetu je IPv4. Kod IPv4 adresiranja, IP adresa je binarni broj veličine 32 bita ali se često zapisuje u decimalnom obliku na način da se 32-bitni broj podijeli na četiri broja od 8 bitova koji se odvajaju točkom. Primjer zapisa IP adrese u binarnom obliku je 11000000.10101000.00000001.00000011, dok bi ta adresa u decimalnom obliku bila zapisana ovako: 192.168.1.3.

Različite mrežne arhitekture podržavaju različite maksimalne jedinice prijenosa (engl. maximum transfer unit – MTU). Ukoliko je MTU veći od dužine IP paketa, paket nastavlja sa prijenosom. No, ukoliko je MTU manji od IP paketa, paket se mora podijeliti na manje jedinice, odnosno fragmente. Nakon što fragmenti dođu do odredišta, ponovno se sastavljaju. Da bi proces fragmentacije bio uspješan, odredišni IP mora biti u mogućnosti razlikovati fragmentirane i ne fragmantirane pakete, koji fragmenti pripadaju kojem paketu, koliki je broj fragmenata i kojim se redoslijedom sastavljaju. Radnje potrebne za sastavljanje fragmenata omogućavaju polja

[9] Mujarić, Eldis. 2009. „Računalne mreže“. Layer-x. http://mreze.layer-x.com/s030100-0.html
[10] Ibid.

Identifikacija, Kontrolne zastavice i Odmak fragmenata. Navedena polja dio su zaglavlja fragmenta (engl. Fragment header) koje je vrlo slično zaglavlju IP paketa.[11]

Opći zadatak Internet protokola je prenošenje informacija s izvora do odredišta. Informacije se prenose kao paketi koji moraju biti adresirani, te ukoliko je potrebno i fragmentirani. Proces prenošenja informacija može biti jednostavan ili kompleksan, ovisno o neposrednoj blizini izvorišnih i odredišnih uređaja. Proces usmjeravanja se obično dijeli na dvije različite vrste, ovisno o tome nalaze li se izvorišni i odredišni uređaji na istoj lokalnoj mreži ili ne:[12]

- Direktno usmjeravanje (eng. Direct Route): Kada se šalju paketi sa jednog na drugi uređaj na istoj fizičkoj mreži, moguće je da se paketi dostave direktno sa izvorišta na odredište.

- Indirektno usmjeravanje (eng. Indirect Route): Kada se dva uređaja ne nalaze na istoj fizičkoj mreži, slanje paketa sa jednog uređaja na drugi naziva se indirektnim.

3. INTERNET PROTOKOL VERIZIJE 6

Godine 1981., objavljen je Internet protokol verzije 4 kao sustav adresa koji se koristi za identificiranje uređaja na mreži. Zbog nestajanja IPv4 adresnog prostora, IETF (Internet Engineering Task Force) započinje sa razvijanjem novog IP protokola – Internet protokola verzije 6. Svrha IPv6 protokola je osiguravanje većeg broja adresnog prostora te otklanjanje ostalih nedostataka IPv4 protokola.

3.1. IPv6 ADRESIRANJE

Jedna od najvećih razlika IPv6 protokola u odnosu na IPv4 protokol je dužina IP adrese. Adrese IPv6 protokola veličine su 128 bita, iz čega proizlazi da postoji 2^{128} različitih IP adresa. Adresa je podijeljena na dva logička dijela od kojih je jedan 64-bitni dio mrežni dio, dok je drugi 64-bitni dio rezerviran za domaćina. Primjer zapisa IPv6 adrese u binarnom obliku:

[11] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd, Kompjuter Biblioteka, 2004. str. 540
[12] https://docs.oracle.com/cd/E26505_01/html/E27061/gcvjj.html

0010000000000001.0000110110111000.0000000000000000.0000000000000000.
0000000000000000.0000000001010010.0000000000000000.0000000000000001

IPv6 adresa zapisuje se kao osam grupa razdvojenih dvotočkom, a svaka je grupa sačinjena od četveroznamenkastog broja zapisanog u heksadecimalnom obliku, kao na primjer:

2001:0DB8:0000:0000:0000:0052:0000:0001

Adrese se mogu pojednostaviti i na način da se nule, koje se nalaze na početku neke od četveroznamenkastih grupa, ne zapisuju. Na primjer, prethodno navedenu adresu možemo zapisati i ovako:

2001:DB8:0:0:0:52:0:1

Za one adrese koje sadrže velik broj nula koristi se skraćena notacija u kojoj se umjesto grupe od četiri nule pišu dvije dvotočke (::). Gore navedena adresa može se zapisati i ovako:

2001:DB8::52:0:1

3.1.1. TIPOVI IPv6 ADRESA

IPv6 adrese dijele se na tri osnovna tipa adresa:

1. Unicast adrese
2. Multicast adrese
3. Anycast adrese

Za razliku od IPv4 protokola, IPv6 protokol nema broadcast adresa koje su izbačene zbog problema sa učestalim nepotrebnim korištenjem univerzalnih paketa koji nisu namjenjeni uređajima te zbog opterećivanja uređaja na mreži. U IPv6, anycast adrese zamijenile su broadcast adrese.

Unicast adrese

Postoji nekoliko vrsta na koje se dijele IPv6 unicast adrese: [13]

1. **Agregabilna globalna jedinstvena adresa (eng. Aggregatable Global Unicast Address):** Jednaka je IPv4 javnoj adresi i namijenjena je za globalno usmjeravanje.
2. **Jedinstvena adresa lokalne mreže (eng. Unicast site-local address):** Slična je privatnoj IPv4 adresi. Nakon prva 48 bita dijeli istu strukturu kao globalna jedinstvena adresa. Prefiks jedinstvene adrese lokalne mreže je FEC0::/48 i zauzima 48 bita. Polje Identifikator podmreže zauzima 16 bitova i omogućuje 65 536 podmreža. Zadnje polje je identifikator sučelja koje zauzima 64 bita.
3. **Jedinstvena adresa lokalne veze (eng. Unicast link-local address):** Domaćini na istoj podmreži koriste automatski kofigurirane adrese za međusobno komuniciranje. Prefiks ove adrese je FE80::/64 i zauzima 64 bita. Ostalih 64 bita zauzima polje Identifikator sučelja.
4. **Multicast adrese:** Multicast adrese IPv6 protokola slične su multicast adresama IPv4 protokola. Adresirani paketi dostavljaju se na sva sučelja koja ta adresa identificira.

8 bitova	4 bita	4 bita	112 bitova
1111 1111	Kontrolne zastavice	Raspon	Identifikator grupe

Tablica 1: Format IPv6 multicast adrese

Izvor: https://technet.microsoft.com/ptpt/library/cc757359(v=ws.10).aspx

Prvo polje označava prefiks multicast adrese i uvijek iznosi 1111 1111. Drugo polje dužine je 4 bita od kojih su prva 3 bita 0. Ukoliko i posljednji bit iznosi 0, označava adresu kao trajno dodijeljenu multicast adresu. Ukoliko je postavljeno na 1, označava prolaznu adresu, odnosno adresu koja nije trajno dodijeljena. Treće polje označava raspon multicast adresa i moguće je šesnaest različitih vrijednosti u rasponu od

[13] https://www.carnet.hr/tematski/ipv6/adresiranje.html

0 do 15. Četvrto polje označava određenu multicast grupu unutar svake razine raspona.

Anycast adrese

Anycast adresa je adresa dodijeljena setu sučelja koji obično pripadaju različitim čvorovima. Paket koji je poslan anycast adresi dostavlja se najbližem sučelju kojeg je anycast adresa identificirala. Anycast adresa se sintaktički ne razlikuje od unicast adrese jer se dodjeljuju iz adresnog prostora unicast adrese. Dodjeljivanje unicast adrese većem broju sučelja čini unicast adresu anycast adresom, no čvorovi na koje se adresa dodjeljuje moraju biti konfigurirani na način da prepoznaju da je to anycast adresa. Anycast adresa se ne smije korisiti kao izvorišna adresa IPv6 paketa i ne može ju koristiti domaćin, već samo uređaj.[14]

3.2. Zaglavlje ipv6 paketa

U odnosu na zaglavlje IPv4 protokola, zaglavlje IPv6 protokola mnogo je jednostavnije jer su izbačena polja koja se ne koriste često ili su zastarjela. U zamjenu za njih, dodana su polja koja omogućuju bolju podršku prometu u stvarnom vremenu.

<table>
<tr><td colspan="2">Verzija</td><td>Prioritet paketa</td><td colspan="2">Oznaka toka</td></tr>
<tr><td colspan="3">Duljina korisnih informacija</td><td>Sljedeće zaglavlje</td><td>Broj skokova</td></tr>
<tr><td colspan="5">Izvorišna adresa</td></tr>
<tr><td colspan="5">Odredišna adresa</td></tr>
</table>

Tablica 2: Format zaglavlja IPv6 protokola

Izvor: http://www.itprotoday.com/management-mobility/what-ipv6-header-format

Verzija (engl. Version): Ovo je polje duljine 4 bita i sadrži broj 6 što označava verziju protokola. U zaglavlju IPv4 paketa nalazi se broj 4 koji označava taj protokol.

Prioritet paketa (engl. Packet priority): Polje prioritet paketa zauzima 8 bitova u IPv6 zaglavlju i koristi se za kontroliranje zagušenja. Prioriteti se određuju na način da se značajniji paketi prikazuju višim vrijednostima. Vrijednosti prioriteta obilježavaju

[14] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3se/5700/ip6-anycast-add-xe.html

se brojevima od 0 do 7. Nulom su označeni paketi čija su kašnjenja prihvatljivija dok su sedmicom označeni paketi čija su kašnjenja neprihvatljiva.[15]

Oznaka toka (engl. Flow label): Ovo polje zauzima 20 bitova i koristi se sa poljem Prioritet paketa. Prenošenje paketa koji pripadaju istome slijedu na sličan način obavlja usmjernik. Informacije koje su dio određenog slijeda određuju se same u sklopu paketa ili se pak prenose pomoću kontrole protoka kao što jebRSVP (engl. Resource reSerVation Protocol).

Duljina korisnih informacija (engl. Payload lenght): Označava duljinu korisnih informacija i zauzima 16 bitova. Koristi se kako bi usmjerivači prepoznali koliko infromacija paket može sadržavati ili sadrži. Ovo je polje postavljeno na 0 i zamjenjuje polje duljina zaglavlja kod IPv4 zaglavlja.

Sljedeće zaglavlje (engl. Next header): Ovo polje zauzima 8 bitova, zamjenjuje polje protokol u IPv4 zaglavlju i jedan je od najvažnijih dodataka kod IPv6 zaglavlja. Kada IPv6 paket koristi dodatna zaglavlja, tada polje sadrži identifikator prvog zaglavlja proširenja, koje koristi svoje vlastito polje sljedeće zaglavlje koje također sadrži identifikator sljedećeg zaglavlja itd.

Broj skokova (engl. Hop limit): Zamjena je za polje Vrijeme života u zaglavlju IPv4 protokola. Vrijednost ovog polja smanjuje se za 1 nakon prolaska kroz uređaj koji ga preusmjerava dalje. Kada vrijednost dođe na nulu, paket se odbacuje. Glavna zadaća ovog polja je identificirati i odbaciti pakete koji su zapeli u beskonačnoj petlji prilikom grešaka u usmjeravanju. Najveća moguća vrijednost polja iznosi 255 skokova, što znači da paket može proći kroz najviše 254 usmjerivača prije nego bude odbačen.

Izvorišna adresa (engl. Source address): Ovo polje sadrži 128-bitnu IP adresu koja, kao i kod IPv4 zaglavlja, predstavlja uređaj sa kojeg se paket šalje.

Odredišna adresa (engl. Destination address): Sadrži 128-bitnu IP adresu uređaja na koji se paket šalje.

Nekoliko je razlika što se tiče polja u zaglavlju kod IPv4 protokola u odnosu na zaglavlje IPv6 protokola. Dva su polja samo preimenovana: polje broj skokova se kod

[15] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd, Kompjuter Biblioteka, 2004. str. 562

IPv4 zaglavlja naziva vrijeme života, a polje Tip servisa se kod IPv6 naziva prioritet paketa. Dva se polja koriste u slične svrhe kao i polja IPv4 zaglavlja, ali su malo izmijenjena i preimenovana. Ta su polja duljina korisnih informacija i sljedeće zaglavlje koja se u IPv4 zaglavlju nazivaju duljna zaglavlja i protokol. U zaglavlje IPv6 protokola nadodano je polje oznaka toka, a uklonjena su polja identifikacija, kontrolne zastavice i odmak fragmenata jer se fragmentacija koristi rijeđe nego u IPv4 protokolu. Ukoliko je fragmentacija potrebna, ova se polja nalaze u dodatnim zaglavljima. Uklonjeno je i polje cheksum. [16]

3.2.1 Dodatna zaglavlja IPv6 paketa

Dodatna zaglavlja IPv6 protokola sadržavaju dodatne informacije koje koriste mrežni uređaji kao što su usmjerivači, prekidači i domaćin krajnjeg računala kako bi odlučili na koji način obraditi ili usmjeriti IPv6 paket. Sva polja koja su potrebna isključivo za posebne namjene nalaze se u dodatnim zaglavljima, što omogućuje da se smanji veličina osnovnog zaglavlja i da sadrži samo ona polja koja se koriste cijelo vrijeme. Svako zaglavlje nakon kojega slijedi dodatno zaglavlje mora u polju sljedeće zaglavlje sadržavati vrijednost koja upućuje na vrstu dodatnog zaglavlja. Postoji šest različitih tipova dodatnih zaglavlja:

1. Zaglavlje sa opcijama za pojedinačne skokove (engl. Hop-by-Hop Options)
2. Zaglavlje sa opcijama za odredište (engl. Destination Options)
3. Zaglavlje za usmjeravanje (engl. Routing)
4. Zaglavlje fragmentacije (engl. Fragment)
5. Zaglavlje za provjeru autentičnosti (engl. Authentication)

Enkapsulacija sigurnosti nosivog tereta (engl. Encapsulating security Payload)

Zaglavlje sa opcijama za pojedinačne skokove: Ukoliko se koristi ovo dodatno zaglavlje, vrijednost u polju sljedeće zaglavlje u osnovnom zaglavlju iznositi će 0. Duljina ovog zaglavlja je varijabilna i ono određuje parametre isporuke na svakom skoku na putu do odredišnog računala. Ako se koristi ova opcija za pojedinačne

[16] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no starch press, 2005. str. 407

skokove, mora biti prvo po redu od dodatnih zaglavlja, odmah nakon osnovnog zaglavlja.[17]

Zaglavlje sa opcijama za odredište: Određuje parametre isporuke paketa za srednja odredišna računala ili za krajnjeg odredišnog domaćina. Ukoliko paket koristi ovu opciju, vrijednost polja sljedeće zaglavlje na prijašnjem zaglavlju mora biti 60. Duljina ovog zaglavlja je varijabilna.

Zaglavlje za usmjeravanje: Dodatno zaglavlje za usmjeravanje koristi se za izvođenje izvorišnog usmjeravanja u IPv6 protokolu. Određuje metodu koja izvorišnom uređaju dopušta da odredi rutu paketa. Ako se koristi dodatno zaglavlje za usmjeravanje, tada se u polju sljedeće zaglavlje mora nalaziti vrijednost 43.[18]

Sljedeće zaglavlje	Duljina dodatnog zaglavlja	Tip usmjeravanja (=0)	Broj segmenata koji slijede
Rezervirano			
Adresa 1 (128 bita)			
Adresa N (128 bita)			

Tablica 3: Format dodatnog zaglavlja za usmjeravanje
Izvor: Charles M. Kazierok., The TCP/IP Guide

Zaglavlje fragmentacije: Ovo dodatno zaglavlje određuje kako izvršiti fragmentaciju i usluge ponovnog sastavljanja. Ukoliko paket koristi dodatno zaglavlje fragmentacije, u polju sljedeće zaglavlje nalazi se vrijednost 44. Duljina zaglavlja iznosi 8 bitova.

Sljedeće zaglavlje	Rezervirano	Odmak fragmenata	Rezervirano	Više fragmenata
Identifikacija				

Tablica 4: Format dodatnog zaglavlja fragmentacije
Izvor: Charles M. Kazierok., The TCP/IP Guide

[17] „Understanding IPv6 Packet Header Extensions“.2017. TechLibrary. https://www.juniper.net/documentation/en_US/junos/topics/concept/ipv6-flow-extention-headers-understanding.html
[18] Ibid.

Zaglavlje za provjeru autentičnosti: Duljina ovog zaglavlja je varijabilna, a ukoliko paket koristi zaglavlje za provjeru autentičnosti, vrijednost u polju sljedeće zaglavlje biti će 51. Ovo zaglavlje pruža autentičnost, integritet podataka i zaštitu protiv ponavljanja.

Enkapsulacija sigurnosti nosivog tereta: Pruža autentičnost i povjerljivost podataka za pakete koji koriste ovo zaglavlje. Ukoliko paket koristi ovo dodatno zaglavlje, vrijednost u polju sljedeće zaglavlje biti će 50, dok je duljina samog zaglavlja varijabilna.[19]

4. Internet STVARI (IoT)

„Pojam internet stvari ima mnogo različitih definicija, a jedna od njih glasi da je to računalni koncept koji opisuje ideju gdje se svakodnevni fizički objekti povezuju na internet te prikupljaju, razmjenjuju i pohranjuju podatke sa ostalim uređajima i ljudima na temelju prikupljenih podataka.“[20] Različiti objekti kao što su senzori, pametni uređaji, uređaji za pohranu podataka, uređaji za komunikaciju s korisnicima, aktivno sudjeluju u komunikaciji. Komunikacija se ne vrši između ljudi, nego samih objekata koji samostalno stvaraju, razmjenjuju i koriste podatke.

4.1. Primjena IoT-a

Internet stvari (IoT) predstavlja mrežu ugradbenih uređaja koji sadržavaju senzore, aktuatore i mrežnu karticu pomoću koje je omogućeno povezivanje i razmjena podataka u nekom fizičkom objektu putem već postojeće Internet infrastrukture. Stvari ili objekti koji pripadaju IoT-u su bilo koji fizički objekti iz stvarnog svijeta. To mogu biti strojevi, procesi, uređaji, zgrade i drugo. Da bi neki objekt bio pametan on mora imati jedinstveni identifikator, mogućnost komuniciranja i mogućnost kontrole. CSM (Cyber Phisical System) sustav služi za transformiranje prikupljenih podataka u informacije s kojima će u stvarnom svijetu biti moguće prikupljanje različitih podataka koji služe optimizaciji. Osim IoT-a postoji i WoT (Web of Things) koji služi kao aplikacijski sloj za IoT.

[19] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no starch press, 2005. str. 409
[20] „Internet of Things“. Techopedia.https://www.techopedia.com/definition/28247/internet-of-things-iot

Primjena IoT-a je raznovrsna, a najčešće se primjenjuje u:

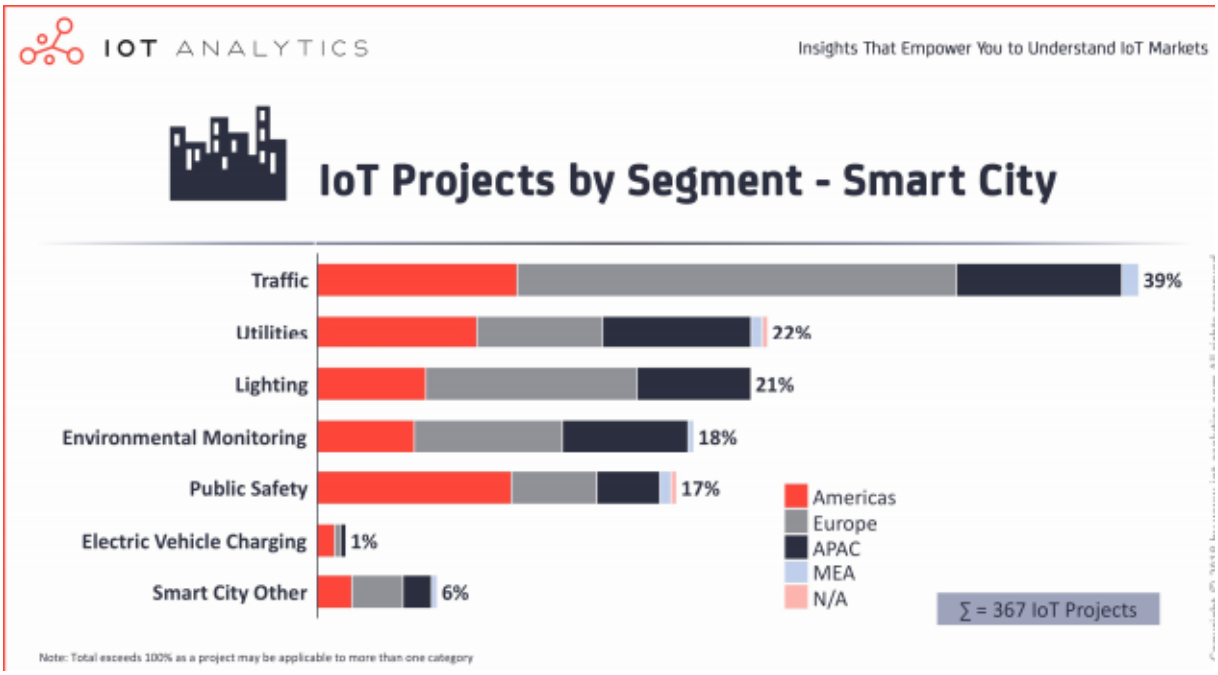
1. Potrošačke svrhe
2. Poslovne
3. Infrastrukturne
4. Industrijske

Potrošačke su namjenjene krajnim korisnicima kod kojih se primjenjuju na pametne kuće (kao što je redukcija troškova, asistent tehnologija za nepokretne, detekcija pada kod starijih osoba). Danas na tržištu postoje veći broj sustava koji pomažu u regulaciji različitih potreba korisnika, sve od mjerenja potrošnje struje pa do alarm sustava i pametnih brava.

Infrakstrukturne IoT primjene su kod „pametnih“ gradova gdje su svi senzori umreženi sa konstantnim tokom podataka. Iako takav sustav još nije u primjeni velikog broja gradova, postoji dovoljno primjera da se mogu pratiti rezultati svih senzora koji postoje u nekom gradu te u budućnosti primijeniti možda takav ili sličan sustav na svoje područje. Gradovi koji vec koriste IoT su Santander u Španjolskoj gdje postoji deset tisuća različitih senzora koji olakšavaju sve potrebe svojih građana kao što je pronalaženje slobodnog parkirnog mjesta, praćenje okoliša, prometa i drugo.

Također, u New Yorku postoji pametno upravljanje prometom u kojem su umrežena i prate se sva gradska plovila uživo 24/7. Na taj se način štedi energija, bolje se upravlja flotom, građanima je dostupan besplatan javni Wi-Fi i beskontaktno plaćanje karata. Neke od primjena senzora u gradovima mogu biti:

1. Praćenje napunjenosti spremnika za otpad (Smart urban waste management)
2. Praćenje sveukupnog stanja u gradu kao što su buka, kvaliteta zraka, nezgode i drugo (Smart urban planning)
3. Fokusiranje na efikasniju navigaciju i smanjenje gradskih gužvi (Intelligent commuter)
4. Praćenje stanja okoliša na velikim površinama (npr., kvaliteta zraka, ispravnost vode, stanje tla, prirodne katastrofe, šume, životinjski svijet)
5. Praćenje i kontrola stanja infrastrukture (npr., kvaliteta mostova, tračnica na željezničkoj pruzi, vjetroelekrane, solarne elektrane)



Slika 2: IoT projekti po segmentima

Izvor: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

Industrijska primjena IoT-a (IIoT) koristi se kod praćenja opreme, proizvodnje, procesa, stanja strojeva (previđanje kvarova), perosnalizirane proizvodnje, bolje prilagodbe potražnji (proizvodnja, strojevi, lanac opskrbe), pomoću RFID tehnologije tagiraju se proizvodi u skladištu na način da se identificiraju i lociraju tzv. Smart Product Managemet. Smart Grids služi za optimizaciju proizvodnje energije prema potrebama koje se događaju u stvarnom vremenu. IoT sustavi pomažu i kod transporta i logistike na način da vrše integraciju komunikacije, kontrole i obrade informacija između različitih transportnih sustava. Moguće su i primjene u svim aspektima transportnog sustava (vozilo/ infrastruktura/vozač) kao što je komunikacija između vozila, pametna kontrola prometa, pametna naplata cestarine, autonomno upravljanje vozilom i drugo.

Osim u ove četiri glavne primjene postoje i druge grane u koje se polako uvodi IoT tehnologija. Možda najbolja primjena je u poljoprivredi gdje bi proizvođači hrane mogli povećati doprinose na način da pomoću sustava konstantno prate stanje svojih biljaka i tla te po potrebi daju biljkama i tlu ono što je u tom trenutku potrebno za bolji rast i razvoj. Također, ovdje su vrlo korisni i senzori sa praćenje vremenskih uvjeta kako bi se moglo unaprijed upozoriti poljoprivrednika o nadolazećim promjenama

vremena. Koristi se i u medicini gdje se prate pacijenti na udaljenostima i notificiraju hitne situacije. Može se primijeniti kontinuirana medicinska njega umjesto rutinskih posjeta liječniku, kod kuće bolesnik ima medicinske uređaje koji prate zdravstveno stanje (tlakomjer, ekg monitor i drugo), pametni kreveti koji se namještaju prema pacijentu ili pak pametne vage.

Senzori koji se primjenjuju u fitnesu su praćenje svih aktivnosti koje korisnik izvodi kao što je trajanje same aktivnosti, brojanje koraka, srčana frekvencija, temperatura tijela, znojenje, praćenje sna i krvnog tlaka te tjelesne mase.

Intelligent Shopping je vrsta IoT-a koji se probija na tržište u trgovinama. Radi na principu RFID tehnologije gdje su svi proizvodi označeni, imaju proširenu stvarnost, postoje personalizirani oglasi i sve to bez blagajne. Još jedan sustav se koristi, možda i napredniji od prije navedenog kod koje se ne koristi RFID tehnologija već postoji mnoštvo kamera koje detektiraju gdje je korisnik nešto uzeo. Takav sustav koristi Amazon Go. Sustav radi na način da morate imati tri stvari: pametni telefon, Amazon aplikaciju i Amazon račun. Nakon ulaska u trgovinu skenira se vlastiti QR kod prema kojem se zna tko je kupac i njegov račun. Ne postoje blagajne te je izlaz slobodan.

Slika 3: Prikaz funkcioniranja Amazon Go tehnolgije

Izvor: https://www.digitalpulse.pwc.com.au/amazon-go-strategy-retail-grocery/

Zbog velikog broja IoT uređaja raste i potreba za pohranom podataka u oblak. Velike potrebe postoje i za obradom prikupljenih podataka i brzinom obrade zbog velike količine IoT podataka. Svi podaci su otvorenog tipa tako da i drugi korisnici mogu razvijati svoje aplikacije i usluge na već postojećim tuđim podacima.

4.2.1. Prednosti i mane Internet stvari

Idealističke pretpostavke kako bi mogao IoT funkcionirati u budućnosti su[21] :

1. Sveprisutna mreža (Internet)
2. Neprekinutost konekcije
3. Gotovo besplatno procesiranje prodataka
4. Velika propusnost kanala
5. Dostupnost električne energije
6. Neograničena pohrana podataka

Rizici koje donose takvi sustavi mogu biti:

1. društveni
2. tehnički
3. ekološki

Društveni rizici događaju se oko slobode izbora (IoT sustav odlučuje umjesto nas), gubi se privatnost i nastaje politička manipulacija na način da se kontroliraju IoT sustavi od strane vlade i drugih.

Tehnički rizici manifestiraju se u previše senzora ili IoT sustava na jednom mjestu pa im se gubi smisao i velika potrošnja električne energije jer puno IoT uređaja troši i puno energije, problem može biti i kod bučnih punjača i skladištenja baterija nakon prestanka upotrebe)

Ekološki rizici nastaju kada se IoT sustavi prestanu koristiti jer elektroničke komponente koje su ugrađene u takve sustave danas je teško reciklirati jer sadrže teške metale i toksične materijale). Problem kod IoT sustava je i taj da ima potrebu

[21] „The advantages and disadvantages of Internet Of Things“. 2016. E27. https://e27.co/advantages-disadvantages-internet-things-20160615/

za stalnim ažuriranjem (svakih 5 god) dok klasične utični, prekidači i ostala tehnologija koja je danas vrlo raširena traje i do 50 godina u kućanstvima.

4.1.2. Komunikacija IoT uređaja

Postoje sljedeće dvije vrste načina komunikacije IoT uređaja:

Stroj sa strojem (M2M) - različiti privatni protokoli sa podacima koji su često pomješani sa protokolom. U budućnosti će se koristiti najviše komunikacija preko oblaka (engl. cloud).

Stroj sa ljudima (M2H) - komunikacija se izvršava na način da se obrađuju podaci u informacije za krajnjeg korisnika na temelju kojih se pružaju različite funkcionalnosti.

4.2. Tehnologija IoT-a

Iot tehnologija je spoj više tehnologija u jedno. Kod sustava imamo Konvergenciju jeftinih ugradbenih sustava, jeftinih senzora, bežičnu komunikaciju, širokopojasni Internet i označavanje objekata. Komponente samog sustava su ugradbeni mikroprocesor, memorija, senzori, aktuatori, mrežna oprema, pristupnici i poslužitelj za oblak. Moguće je povezati sustave sa bilo kojim oblakom koji je dostupan kao što su Google Cloud Platform, Microsoft Azure, Amazon Web Service i drugi.

Sam softverski dio sastoji se operacijskog sustava, podatkovne baze i aplikacije. Postoji više vrsta sustava za prototipiranje, neki od njih su Arduino Uno, Raspeberry Pi te BeagelBone Black.

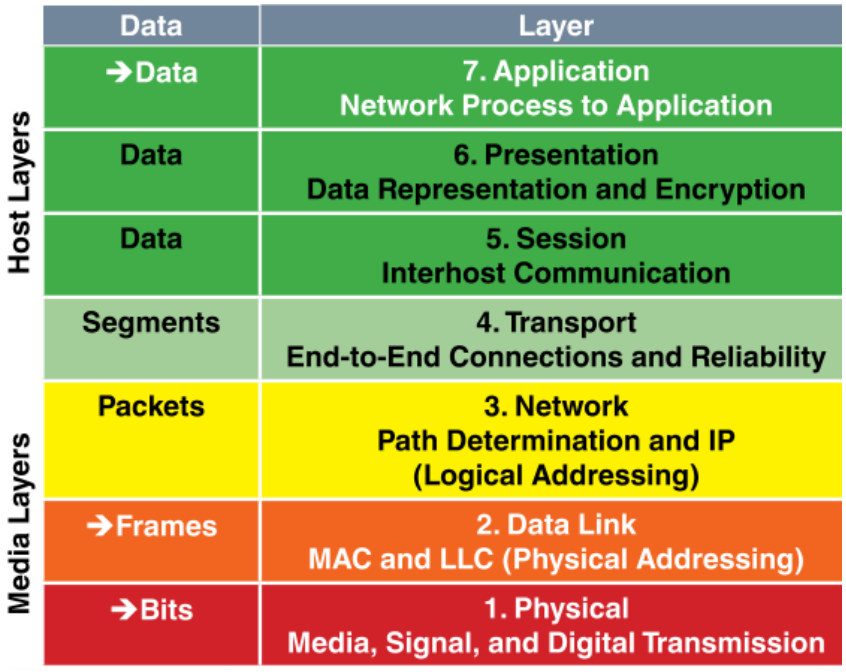
Kod identifikacije objekata koriste se tehnologije:

1. RFID
2. NFC
3. Barcodes & QR code
4. Digital Watermarking

Adresiranje je moguće pomoću URI, URL ili IP adrese kod kojih se najprije koristio IPv4 protokol. No, danas se koristi IPv6 protokol s kojim je omogućen veći adresni prostor, autokonfiguriranje i 6LoWPAN kompresija zaglavlja. 6LoWPAN je tehnologija koja koristi IPv6 Internet protokol unutar LR-WPAN mreže.

4.3. Bežične i žičane IoT tehnologije

Ideja umrežavanja nastala je 1965. godine gdje su pojedinci imali ideju povezati nezavisna računala u umrežena računala koja su bila na različitim mjestima. Sama definicija umrežavanja bila bi prijenos podataka, datoteka ili naredbi između međusobno neovisnih računala. Sredinom 1980-ih godina standardiziran je OSI model na način da su mreže podijeljene u slojeve. Unutar OSI modela događa se enkapsulacija podataka gdje se podaci iz prethodnog sloja omataju dodatnim podacima iz novog sloja. OSI model[22] podijeljen je na aplikacijski i transportni sloj. Prva tri sloja čine aplikacijski, a donja četiri čine transportni sloj.



Slika 4: Komunikacijski slojevi OSI modela

Izvor: https://instrumentationtools.com/7-osi-layers-of-communications/

[22] „Računalne mreže – OSI referentni model“. 2008. Sys.portal Carnet.https://sysportal.carnet.hr/node/352

Mrežne tehnologije koje služe za komuniciranje još su uvijek na samom početku razvoja i mogu biti vrlo važne kod IoT primjene kao što je kod pametnih gradova gdje sve mora biti umreženo da bi savršeno funkcioniralo i da bi imali stvarne rezultate i informacije o nekoj pojavi ili događaju. Između različitih vrsta tehnogija postoje razlike u samom dometu unutar kojeg djeluju. Buduće i postojeće bežične tehnologije morale bi omogućiti veliku brzinu prijenosa podataka, učinkovitije korištenje spektra, veliku pokrivenost, visoku sigurnost, robusnost, nisku cijenu i agilne mehanizme šifriranja. Danas se već priča o uvođenju pete generacije tehnologije (5G) koja bi također morala pružiti veće pogodnosti nego što smo ih imali sa nižim generacijama kao što su veće brzine prijenosa, niže troškove i drugo. Ključne tehnologije koje su nam potrebne za daljni razvoj IoT sustava su: LTE, Wi-Fi, LoRaWAN, Bluetooth, ZigBee. Bežične mreže mogu se podijeliti na tri osnovne klase:

1. WPAN
2. WLAN
3. WMAN

WPAN se koristi za povezivanje pojedinih uređaja na mjestu pojedinca kao što je to radno mjesto i koristi IEEE 802.15 standard. U takvu tehnologiju spadaju ZigBee i Bluetooth. WLAN može povezivati dva ili više uređaja međusobno koji nisu previše udaljeni jedan od drugoga. Napoznatija takva tehnologija je Wi-Fi. I treći WMAN koji je zadužen za pokrivanje sa bežičnom mrežom veliko područje, tehnologija se temeljni na point- to-point ili point-to-multipoint mreži. Kod takve mreže postoji samo jedan davatelj koji je najčešće vlada ili tvrtka. Pristup mreži ostvaruje se tek kada se korisnik pretplati na tu uslugu. Tehnologije koje se koriste kod WMAN-a su LTE, LoRaWAN. LoRaWAN je zadužen za pružanje bežične mreže sa niskom potrošnjom energije koji su vrlo bitni kod IoT uređaja koji rade na daljinu i na bateriju bez stalnog pristupa električnoj energiji. Također LoRaWAN pomaže i kod smanjenja same cijene troškova održavanja.

Wi-Fi

Standard 802.11 definiran od IEEE zajednice naziva se još i skraćeno WI-Fi. Bežična mreža koja sliči onoj žičanoj uz jednu razliku, što ovi uređaji ne koriste kablove za povezivanje sa routerima i drugim korisnicima već koriste antene koje se mogu nalaziti van ili unutar samog uređaja.

Da bi nastala Wi-Fi veza potrebno je kreirati pristupnu točku i Wi-Fi klijenta. Pristupna točka ili AP je uređaj koji odašilje signal za klijente koji se žele umrežiti. Danas svi uređaji koji su iz novijeg doba imaju ugrađeno Wi-Fi sučenje. Ukoliko korisnik posjeduje uređaj koji nema ugrađeno sučelje, on se može nadograditi pomoću adaptera.

Kod Wi-Fi tehnologija vrlo su bitni Wi-fi kanali koji se nalaze u frekvencijskom pojasu od 2.4 GHz i nisu jedini koji se nalaze unutar tog pojasa. Ako se prebaci na veću frekvenciju onda se nudi i brži protok samih podataka ali i manji domet. Ukoliko Wi-Fi adapter može koristiti frekvencijske pojaseve od 5 GHz naziva se još i dvopojasni uređaj.

Standardi koji su definirani određuju brzinu i domet same mreže. Iako se standardi stalno unaprijeđuju od prvog standarda. Danas već nailazimo na poteškoće kao što je radi u zagušljivim okolinama. Ukoliko imamo velik broj uređaja na jako malom prostoru stvaraju se interferencije koje su uzrok padu mrežnih kapaciteta. Standardi koji se danas koriste nisu predviđeni za rad na tako zagušljivim okolinama i rješavanju različitih smetnji koje se javljaju u takvom načinu rada.

Wi Fi Direct

Služi direktnoj WiFi vezi bez pristupne točke. Koristi se u svrhu jednostruke komunikacije između dva uređaja. Odličano radi u spajanju s više Wi-Fi uređaja u susjedstvu, a ima puno veći doseg nego Bluetooth. Također podržava i WPA-2 enkripciju.

Bluetooth

Ideja za takvom tehnologijom nastala je 1994. godine u svrhu prijenosa podataka bez žice. Tehnologija je male potrošnje energije koja se koristi za prijenos podataka između dva ili više uređaja. Postoji dvije vrste tehnologije. BluethoothLE koristi se najviše kod IoT tehnologija gdje nema velike količine podataka, a nužno je očuvanje energije. Vrlo je jeftin za implementaciju što je također jedna od bitnih karakteristika kod odabira tehnologije. Osnovni elementi protokola su :

1. Generic Attribute Profile (GATT) – profil za razmjenu malih količina podataka kroz link. Jedan uređaj može imati više GATT profila (npr. jedan za očitanje senzora, drugi za očitanje stanja baterije).
2. Attribute 2. Protocol (ATT) – protokol ispod GATT-a. Svaki atribut se identificira s 128-bitnim UUID (Universally Unique Identifier). Usluge, karakteristike i deskriptori se kolektivno zovu atributi i identificiraju sa UUID.
3. Characteristic – sastoji se od jedne vrijednosti i više deskriptora. Vrlo slično tipu podataka kod klasi.
4. Descriptor – deskriptori opisuju određenu vrijednost karakteristike, npr. mjernu jedinicu „BPM (beats per minute)"
5. Service – usluga je skup karakteristika, npr. primarna usluga „Heart Rate Monitor" sadrži karakteristiku „heart rate measurement" i karakteristiku „time interval between measurements" itd.

ZigBee

Protokol baziran na 802.15.4 IEEE fizičkom i sloju podatkovne veze. Kod IoT tehnologije vrlo je koristan zbog niske potrošnje energije te ima malu podatkovnu propusnost. Domet mu je obično 10-20 metara, ukoliko je potreban veći domet tada se koristi mesh mreža.
Prednost ovog protokola što je jeftiniji od BLE i WiFi uređaja. Osiguran je sa 128-bitnim simetričnim enkripcijskim ključem. [23]

LoRaWAN

LoRaWAN (Low Power WAN Protocol for Internet of Things) je još jedan protokol koji se sastoji od dviju tehnologija. LoRa sadrži podatkovni sloj i primjenjuju se u P2P komunikaciji. LoRaWAN sadrži isti fizički sloj kao i LoRa ali uz fizički ima i mrežni sloj koji joj omogućava slanje informacija bilo kojoj stanici na oblaku. Definira se kao bežična tehnologija koja je razvijena s ciljem slanja podataka sa vrlo malim brzinama i malom potrošnjom energije na velike udaljenosti. Na taj način slanja vrlo je pogodna za IoT sustave gdje se energija čuva i smanjuju se troškovi.

[23] „Zigbee". 2017. IOT Agenda.https://internetofthingsagenda.techtarget.com/definition/ZigBee

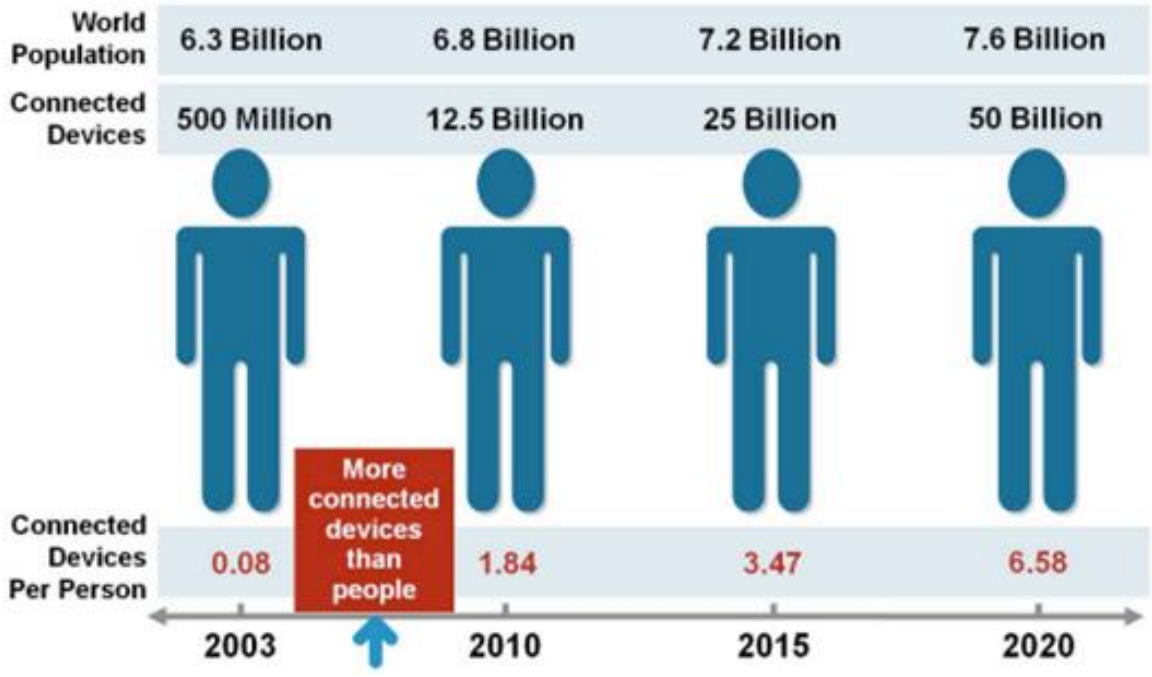
Mreža se sastoji od nekoliko dijelova:

1. Glavni server - upravlja krajnjim točkama i skuplja podatke
2. Mrežni poslužitelj - upravlja mrežom na način da raspoređuje i regulira brzinu prijenosa paketa. Također i uklanja one duple da bi bilo što manje podataka za prijenos
3. Bazna stanica - prima podatke sa glavnih točaka i šalje ih na mrežni poslužitelj pomoću bežične ili žičane mreže

5.IPV6 ZA IoT

5.1. UTJECAJ IPv6 NA IoT

Predviđa se da će do 2030. godine IoT postati „glavni“ grad na tržištu jer već sada ima više od 75% projekata koji pokrivaju ciljeve koji su postavljeni. Mogući razlog takve uspješnosti leži u mogućnosti udaljenog praćenja i kontrole povezanih fizičkih stvari/objekata/usluga koje su do sada bile nepovezane.



Slika 5: Broj uređaja spojenih na Internet u usporedbi sa brojem ljudi na Zemlji

Izvor: https://www.futuristspeaker.com/business-trends/empowering-things-for-our-internet-of-things/

Broj uređaja povezanih na Internet prešao je broj ljudi na Zemlji već 2008. godine. Velike globalne kompanije kao što su Apple i Google ulažu u razvijanje i upotrebu IoT tehnologije. IoT uređaji su već danas postali svakodnevica velikog broja ljudi, a predviđa se da će do 2020. godine broj uređaja povezanih na Internet porasti na 50 milijardi uređaja. IPv4 ima 4,3 milijarde mogućih IP adresa, što je manje od 10% u odnosu na broj uređaja povezanih na Internet koji je predviđen 2020. godine. Jedino rješenje u ovom slučaju je IPv6 koji nudi znatno veći broj IP adresa.

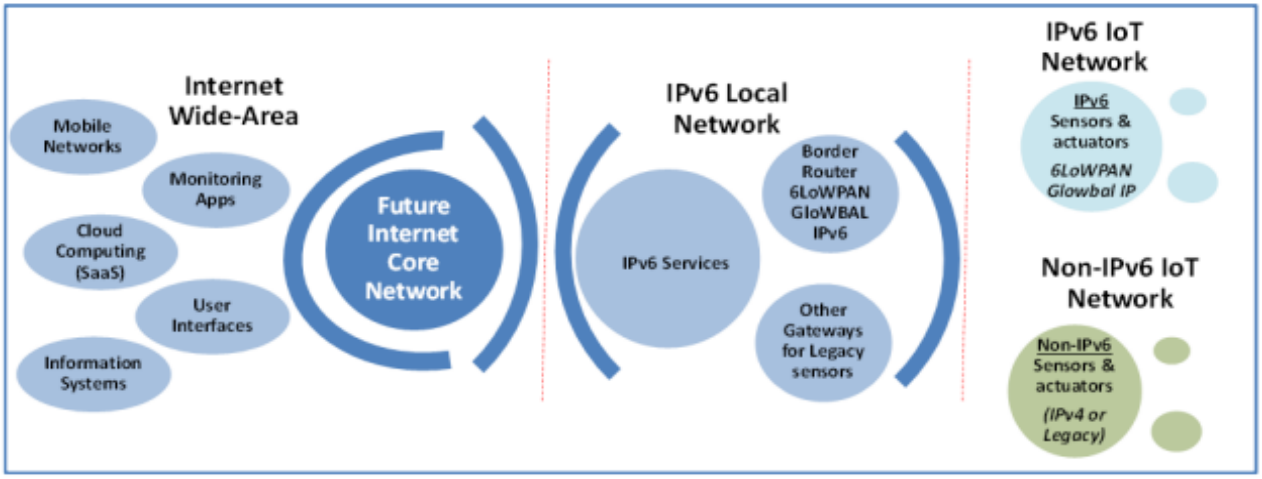
IPv6 donosi Internet stvarima mnogo više od samog adresnog prostora. Sa novim protokolom, IoT može baratati multicast adresama, podržava skalabilnu mobilnost te omogućuje uređajima sa niskom potrošnjom energije ili uređajima na baterije uvrštavanje u nove, efikasnije infrastrukture. Usvajanjem IPv6 drastično se smanjuje rizik od sigurnosnih prijetnji na Internetu. Kompanje koje namjeravaju zarađivati od IoT uređaja, morati će uložiti u prijelaz na IPv6.

5.2. IoT6

IoT6 je trogodišnji istraživački projekt na temu budućnosti Internet stvari. Njegov je cilj iskorištavanje potencijala IPv6 i povezanih standarda za Internet stvari. Glavni ciljevi i izazovi su istraživanje, dizajniranje te razvijanje skalabilne uslužno-orijentiranje arhitekture bazirane na IPv6 kako bi se postigli interoperabilnost, mobilnost te integracija računalstva u oblaku među heterogenim komponentama „pametnih“ stvari, aplikacija i usluga.

5.2.1. IoT6 arhitektura

Cilj IoT6 arhitekture je omogućiti uslužno-orijentiranoj arhitekturi zasnovanoj na IPv6 postizanje interoperabilnosti između različitih komunikacijskih tehnologija te interakciju sa uslugama temeljenima na aplikacijama. Nije jedini cilj korištenje IPv6 protokola samo kao transportni protokol, već i iskoristiti ugrađene značajke IPv6 protokola kako bi se omogućile već implementirane mogućnosti koristeći protokole viših slojeva.



Slika 6: IoT6 arhitektura koja ukazuje na mrežne domene

Izvor: http://www.intercomms.net/issue-20/ipv6-1.html

Slika 6 prikazuje dva različita tipa uređaja: uređaje kompatibilne sa IoT6 i one koji nisu kompatibilni sa IoT6. Uređaji kompatibilni sa IoT6 mogu biti IoT uređaji bazirani na IPv6 ili na protokolima kao što su 6LoWPAN ili CoAP protokoli koji su opisani u sljedećem potpoglavlju. Oni uređaji koji su nekompatibilni sa IoT6 su uređaji koji ne koriste IP komunikacijske protokole ili pak uređaji koji se baziraju na IPv4. Takvi uređaji zahtjevaju da su pristupnici povezani na ostatak IoT6 sustava kako bi protokole, funkcionalnosti te adresiranje prilagodili sa IPv6 preko transparentnih mehanizama. IoT6 LAN mreža IoT uređajima pruža mehanizme povezivanja uzimajući u obzir njihove specifične protokole i tehnologije te ih omogućuje ostatku IPv6 okruženja. IoT6 WAN mreža omogućuje povezivanje višestrukih IoT6 LAN mreža i IoT6 backend poslužitelja te na taj način stvara IoT6 temeljnu infrastrukturu.[24]

5.3. Povezani standardi

Internet stvari zahtjevaju arhitekture softvera koje su u mogućnosti nositi se sa velikom količinom podataka i zahtjevima. Postojeći Internet protokoli kao što su HTTP i TCP protokol nisu optimizirani za komunikaciju niske potrošnje koju IoT uređaji zahtjevaju. Zajedničkim snagama, različita tijela za standardizaciju IEEE i IETF organizacija, su 2003. godine započela sa sastavljanjem okvira komunikacijskih protokola za IoT uređaje. Definirani su protokoli na različitim slojevima LLN stoga,

[24] Alex Galis, Anastasius Gavras., The Future Internet., Springer Open., 2013., str. 165

uključujući 6LoWPAN sloj adaptacije, RPL protokol usmjeravanja te CoAP protokol web prijenosa.

5.3.1. 6LoWPAN

6LoWPAN je otvoreni standard definiran od strane IETF (Internet Engineering Task Force) organizacije koja definira mnoge standarde na internetu kao što su UDP, TCP i HTTP. Komunikacijski sustavi koriste skup pravila ili standarda za fromatiranje podataka i kontrolu razmjene podataka. 6LoWPAN (IPv6 Low-power wireless Personal Area Network) je ključna tehnologija temeljena na Internet Protokolu. Ovaj mrežni protokol definira mehanizam enkapsulacije i sažimanja zaglavlja. Može se koristiti na mnogim komunikacijskim platformama, uključujući Ethernet, Wi-Fi i 802.15.4. Ključna karakteristika ovog standarda je IPv6 stog, koji je proteklih godina imao vrlo važnu ulogu u omogućavanju Internet stvari. Niska potrošnja energije, čvorovi koji se temelje na Internet protokolu te podrška velikim Mesh mrežama čine 6LowPAN vrlo dobrom opcijom za IoT aplikacije.[25]

Neka od područja u kojima se 6LoWPAN tehnologija može primjenjivati:

- kućna automatizacija i automatizacija zgrada
- automatizacija zdravstva i logistike
- osobno zdravlje i fitnes
- poboljšana energetska učinkovitost
- automatizacija industrije
- praćenje vremenske prognoze u stvarnom vremenu
- automatizacija automobila

Arhitetkura 6LoWPAN sačinjena je od bežičnih mrežnih područja niske potrošnje, koji se nazivaju LoWPAN. LoWPAN je skup 6LoWPAN čvorova koji dijele zajednički prefiks IPv6 adrese, što znači da IPv6 adresa ostaje ista neovisno o tome gdje se nalazi čvor na LoWPAN mreži. LoWPAN se sa ostalim IP mrežama spaja putem edge usmjerivača. Neke od LoWPAN karakteristika su: mala veličina paketa,

[25] Jonas Olsson., 6LoWPAN demystified, Texas Instruments., 2014., str. 2

podržavaju adrese različitih duljina, niska propusnost, zvjezdasta i mesh topologija, uređaji sa baterijom, niski troškovi, velik broj uređaja.

5.3.2. RPL protokol

RPL (Routing Protocol for LLN) je IPv6 protokol usmjeravanja 2011. godine od strane IETF organizacije sa ciljem da omogući stvaranje interoperabilnih komercijalne uređaje na rastućim tržištima omogućene LLN (Low-power and Lossy Networks) mrežama.[26] Pojavom Internet stvari, predviđa se sveprisutno globalno povezivanje među milijardama uređaja koji se koriste u svakodnevnom životu. Preklapanjem LLN mreža i Internet stvari, RPL je postao protokol usmjeravanja Internet stvari.

Topologija usmjeravanj RPL protokola u obliku je DODAG (Destination-Oriented Directed Acyclic Graph) grafikona. DODAG se sastoji od 3 vrste čvorova:[27]

- DODAG korijen – odgovoran je za inicijalizaciju topologije, postupa kao granični usmjerivać (engl. border router)
- RPL čvor usmjeravanja (engl. RPL Routing node) – uređaj koji je u mogućnosti prosljeđivati i generirati RPL promet.
- RPL list (engl. RPL Leaf node) – uređaj koji se nalazi na kraju topologije. RPL list može biti usmjerivač ili domaćin.

RPL poruke prenose se putem ICMPv6 (Internet Control Message Protocol version 6) kontrolnih poruka. Postoje tri ključne RPL kontrolne poruke:

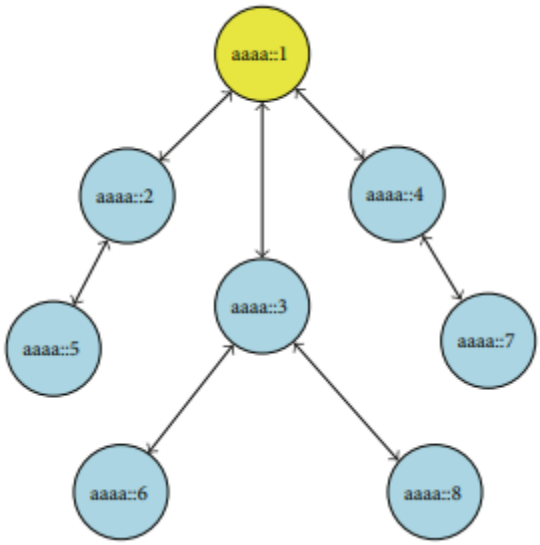
- **DIS** (DODAG Information Solicitation) – ovu poruku čvor šalje susjednim čvorovima kada zahtjeva podatke o usmjeravanju. DIS prikuplja informacije o DODAG objektu sa RPL čvora.

- **DIO** (DODAG Information object) – sadrži informacije koje čvor koristi za otkrivanje RPL instance, određuje parametre konfiguracije.

[26] Oana Iova, Gian Pietro Picco., RPL, the Routing Standard for Internet of Things…Or Is It?., IEEE Communications Magazine, 2016., str. 1
[27] Ines Robles., ROLL on a roll!., IETF Journal., 2018., https://www.ietfjournal.org/roll-on-a-roll/

- **DAO** (DODAG Advertisement Object) – koristi se za prosljeđivanje informacija o destinaciji prema korijenu.

RPL ima dva načina rada: skladištenje i ne skladištenje. Kod skladištenja, paket sa podacima putuje prema gore, sve dok ne dođe do čvora koji sadrži informacije o usmjeravanju do njihove destinacije. Ista se tehnika koristi i kod ne skladištenja, samo što u tom slučaju paket putuje sve do korijena, jedinog čvora koji sadrži informacije o usmjeravanju, prije nego bude preusmjeren prema svojoj destinaciji.



Slika 7: Primjer RPL DODAG grafa gdje svaki čvor ima jedinstvenu IPv6 adresu

Izvor: http://journals.sagepub.com/doi/pdf/10.1155/2013/794326

Slika 7prikazuje RPL DODAG graf gdje svaki čvor ima ID čvora (IPv6 adresa), listu susjednih čvorova te čvor roditelja. Svaki čvor ukazuje na poziciju čvora koji je srodnik ostalim čvorovima.

5.3.3. CoAP protokol

CoAP (Constrained Application Protocol), specijalizirani je transferni protokol koji se koristi sa sa ograničenim čvorovima i ograničenim mrežama kao što je LLN mreža. 6LoWPAN mreža podržava fragmentaciju IPv6 paketa što značajno smanjuje vjerojatnost isporuke. Cilj dizajna CoAP protokola je da ograniči potrenu za fragmentacijom paketa.

Jedan od glavnih ciljeva je dizajniranje općeg protokola koji će omogučiti posebne zahtjeve ograničenih mreža, posebno što se tiče energije, automatizacije izgradnje i ostalih M2M (machine-to-machine) aplikacija.

Model interakcije CoAP protokola sličan je HTTP-ovom klijent-server modelu. M2M interakcija obično rezultira CoAP implementacijom gdje ima ulogu i klijenta i servera. Zahtjev CoAP protokola jednak je onome u HTTP-u gdje ga klijent šalje i zahtjeva neku radnju, a server zatim šalje odgovor.

Definira četiri različite vrste poruka:

1. CON (Confirmable)
2. NON (Non-confirmable)
3. ACK (Acknowledgement)
4. RST (Reset)

Smart home mreža pruža kontrolu i nadgledanje energije kućnih uređaja. Sustavi za kontrolu energije prikupljaju podatke o naponu te trenutne informacije o energiji. Svaki čvor koji prikuplja podatke sa CoAP klijentom mogao bi razmjenjivati podatke sa ostalim čvorovima.

CoAP pomaže u smanjenju povezivanja cloud-uređaja, omogućavajući IoT uređajima da na siguran način šalju podatke na velike udaljenosti koristeći vrlo malo energije.

5.3.4. 6TiSCH

TSCH (Time Slotted Channel Hopping) je MAC (Medium-Access Control) sloj koji je dizajniran na način da podrži široki opseg aplikacija uključujući i one industrijske. Na svojoj jezgri ima tehniku srednjeg pristupa koja koristi vremensku

sinkronizaciju kako bi se ostvarilo djelovanje na niskoj potrošnji jer se time osigurava visoka pouzdanost. Preciznost sinkronizacije utječe na potrošnju energije i može varirati od mikrosekundi do milisekundi.[28]

Kako se usredotočuje isključivo na MAC sloj, to omogućuje da se uklopi u skup IPv6 protokola za LLN mreže (6LoWPAN, RPL i CoAP). TSCH je dizajniran kako bi omogućio optimizaciju i prilagodbu, pojednostavljujući integriranje sa skupom protokola baziranih na IPv6, 6LoWPAN i RPL.

6TiSCH omogućuje upravljanje čvorovima i planiranjem pomoću CoAP sučelja. Također, definira i takozvanu minimalnu konfiguraciju koja mora biti podržana od svih implementacija kako bi ostvarila osnovnu interoperabilnost.

5.4. Sigurnost IPv6

5.4.1. IPSec protokol

Zbog mnogih kritika na temu nedostatka sigurnosti i zaštite na Internetu, IETF (eng. Internet Engineering Task Force) razvio je IPSec protokol. Ovaj je protokol dizajniran kako bi osigurao siguran prijenos paketa. Izvršava se iznad IP protokola i ipod transportnih protokola. IPSec protokol sastoji se od tri glavne komponente:[29]

1. **Zaglavlje autentifikacije (eng. Authentication Header ili AH):** Ova komponenta osigurava autentifikaciju paketa. Može postojati kao jedno od IPv6 zaglavlja ili kao nastavak nakon IPv4 zaglavlja. Zaglavlje autentifikacije sadrži sljedeća polja: Sljedeće zaglavlje (eng. Next Header), Duljina podataka (eng. Payload Length), Rezervirano (eng. Reserved), Sigurnosni parametri (eng. Security Parameters), Broj sekvence (eng. Sequence Number) i Vrijednost provjere integriteta (eng. Integrity Check Value ili ICV).

[28] T. Watteyne, M. Palattella, L. Grieco., Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement., Internet Engineering Task Force., https://tools.ietf.org/html/rfc7554

[29] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd, Kompjuter Biblioteka, 2004. str. 565 i 566

2. **Obvijajući sigurnosni podaci (eng. Encapsulating Security Payload ili ESP):** Ova komponenta povjerljivost osigurava šifriranjem podataka. Šifrirani podaci nalaze se u polju Payload Data.

3. **Protokol za razmjenu ključa:** Jedan od dijelova ove komponente je Internet Security Association and Key Management Protocol (ISAKMP). Ovaj protokol definira formate paketa i pravila za razmjenu paketa u kojima se nalaze informacije o ključu.

6. ZAKLJUČAK

Svakodnevnim povećanjem broja uređaja koji se povezuju na Internet te na taj način komuniciraju, prikupljaju i razmijenjuju podatke, dolazi do potrebe za sve većim brojem IP adresa. Zbog ograničenog broja adresa koje nudi IPv4 protokol, IPv6 po tom pitanju nudi rješenje za Internet stvari.

IPv6 Internet stvarima osim povećanog broja IP adresa nudi i razne druge pogodnosti i mogućnosti kao što su veća sigurnost, mobilnost. Internet stvari zahtjevaju arhitekture softvera koje su u mogućnosti nositi se sa velikom količinom podataka i zahtjevima. IoT uređaji zahtjevaju komunikaciju niske potrošnje te su zbog toga definirani protokoli na različitim slojevima LLN stoga, uključujući 6LoWPAN sloj adaptacije, RPL protokol usmjeravanja te CoAP protokol web prijenosa.

U samo godinu dana, broj IoT uređaja povezanih na internet porastao je sa 5 milijuna na nekoliko milijardi. Mnogo se novaca ulaže u razvoj takvih uređaja i njihov će broj zasigurno i dalje rasti.

LITERATURA

a) Knjige:

1. Kozierok M. C., The TCP/IP Guide, San Francisco: no strach press, 2005.
2. Galis A., Gavras A., The Future Internet., Springer Open., 2013
3. Olsson J., 6LoWPAN demystified, Texas Instruments., 2014
4. Radovan M., Računalne mreže (1), Rijeka, 2010.
5. Shay A W., Savremene Komunikacione tehnologije i mreže, Beograd, Kompjuter Biblioteka, 2004.
6. Wilkins S., „Anatomy of an IPv4 Packet“. Pearson IT Certification, 2012.

b) Web:

1. Mujarić, Eldis. 2009. „Računalne mreže“. Layer-x., URL: http://mreze.layerx.com/s040200-0.html (25.07.2018)
2. Beal, Vangie. 2018. „The 7 Layers of the OSI Model“. Webopedia. https://www.webopedia.com/quick_ref/OSI_Layers.asp
3. http://www.pearsonitcertification.com/articles/article.aspx?p=1843887
4. Oracle Solaris Administration: IP Services URL: https://docs.oracle.com/cd/E26505_01/html/E27061/gcvjj.html (20.07.2018)
5. Adresiranje Internet protokola verzije 6, URL: https://www.carnet.hr/tematski/ipv6/adresiranje.html (25.07.2018)

6. IPv6 Anycast Address, URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3se/5700/ip6-anycast-add-xe.html (25.07.2018)

7. Understanding IPv6 Packet Header Extensions“.2017, TechLibrary. URL:https://www.juniper.net/documentation/en_US/junos/topics/concept/ipv6-flow-extention-headers-understanding.html (01.08.2018)

8. T. Watteyne, M. Palattella, L. Grieco., Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement., Internet Engineering Task Force., url: https://tools.ietf.org/html/rfc7554

9. ZigBee, url: https://internetofthingsagenda.techtarget.com/definition/ZigBee

10. https://sysportal.carnet.hr/node/352

11. https://www.techopedia.com/definition/28247/internet-of-t hings-iot

12. https://e27.co/advantages-disadvantages-internet-things-20160615/

POPIS SLIKA:

POPIS TABLICA: